Quand j'ai couru chanter ma p'tit' chanson pour Marinette
La belle, la trâitresse était allée à l'opéra.
Avec ma p'tit' chanson, j'avais l'air d'un con, ma mère.
Avec ma p'tit' chanson, j'avais l'air d'un con[1].

To Hendrik W. Lenstra, Jr.

DUAL ELLIPTIC PRIMES AND APPLICATIONS TO CYCLOTOMY PRIMALITY PROVING

PREDA MIHĂILESCU

Abstract. Two rational primes p, q are called *dual elliptic* if there is an elliptic curve $E \mod p$ with q points. They were introduced as an interesting means for combining the strengths of the elliptic curve and cyclotomy primality proving algorithms. By extending to elliptic curves some notions of galois theory of rings used in the cyclotomy primality tests, one obtains a new algorithm which has heuristic cubic run time and generates certificates that can be verified in quadratic time.

After the break through of Agrawal, Kayal and Saxena has settled the complexity theoretical problem of primality testing, some interest remains for the practical aspect of state of the art implementable proving algorithms.

1. Introduction

Primality testing is a discipline in which *constructions of objects* in fields of positive characteristic p are mimicked in algebras over rings $\mathbb{Z}/(n \cdot \mathbb{Z})$ for integers n which one believes to be prime, and of whose primality one wishes to have a proof. The constructions should then allow an efficient computation and be based on operations which have the property of either yielding results over $\mathbb{Z}/(n \cdot \mathbb{Z})$ or else display a factor of n or at least a proof of its compositeness.

In the simplest cases, the constructions restrict to simple verifications. Fermat's "small Theorem" stating that $a^{p-1} \equiv 1 \mod p$ for rational primes p and bases a not divisible by p, is the first ingredient used for fast verification of primality of integers n. In the simplest version of the idea, the *Fermat pseudoprime test, to base* a checks $a^{n-1} \equiv 1 \bmod n$ and returns "composite", if the congruence is not verified. If it is verified, only probabilistic statements can be made about primality of n.

Stronger statements are obtained when one has sufficient information about the factorization of $n - 1$. For instance, if there is a prime $q|(n-1)$ and $q > \sqrt{n}$,

[1]Georges Brassens: *Marinette*

Date: Version 2.0 February 2, 2008.

The research was completed while the author is holding a research chair sponsored by the Volkswagen Stiftung.

while $\left(a^{(n-1)/q}-1,n\right)=1$ and $a^{n-1}\equiv 1 \bmod n$, then one easily proves that n is prime. This test constructs a *primitive* $q-$th *root* of unity modulo n, in the sense that $\Phi_q(\alpha)=0 \bmod n$ with $\alpha=a^{(n-1)/q}\text{rem } n$ and $\Phi_q(X)$ the $q-$th cyclotomic polynomial. Tests of this type are known under the name of Lucas - Lehmer tests. They share the feature, that one proves that a certain number $a\in(\mathbb{Z}/n\cdot\mathbb{Z})^*$ is a primitive $q-$th root of unity for some $q>\sqrt{n}$ - so it generates a cyclic subgroup of $(\mathbb{Z}/n\cdot\mathbb{Z})^*$ which is, by its size, incompatible with the hypothesis that n is be composite.

The idea was generalized, freeing it of the requirement for a priori knowledge of large factors of $n-1$. This is made possible by working in larger extensions of $\mathbb{Z}/(n\cdot\mathbb{Z})$ and using more involved properties of rings in cyclotomic fields and the related Gauss and Jacobi sums. The resulting algorithms are currently denoted by the generic name *Cyclotomy Primality Proving* (CPP). They originate in the work of Adleman, Pomerance and Rumeley [1] and were improved by Lenstra et. al. [21], [23], [22], [11], [8], [26]. Their main idea is to building a frame – a Galois algebra over $\mathbb{Z}/(n\cdot\mathbb{Z})$ – in which a factor $\Psi(X)|\Phi_s(X) \bmod n$ can be constructed for some large s and such that, if n is prime, the factor is irreducible. The definitions of the Galois algebras in which the test take place have undergone some variations [8, 26, 30, 25] since their introduction in [23].

The name CPP covers an unconditionally deterministic variant and one which is deterministic under assumption of the ERH, as well as a Jacobi sum and a Lucas - Lehmer variant; all the variants may well be combined together. The CPP test provides a proof of the fact that the $s-$th cyclotomic polynomial $\Phi_s(X)\in\mathbb{Z}[X]$ – for some special, large and highly composite integers s – factors modulo n the way it should, if n were prime. If this is the case, primality of n follows, *or* the existence of some prime factor

$$r\in\{n^i \text{ rem } s : i=1,2,\ldots,t=\text{ord}_s(n)\}. \tag{1}$$

The algorithms of CPP are *de facto* fast, competitive primality proving algorithms, but they have the complexity theoretical intolerable feature of a provable *superpolynomial* run - time

$$O\left(\log(n)^{\log\log\log(n)}\right), \tag{2}$$

which is in fact the expected size of t in (1).

The use of elliptic curves was first proposed for primality proving by Goldwasser and Kilian [18] in an algorithm which was proved to be random polynomial up to a possible, exponentially thin, exceptional set. The algorithm was made computationally practical by Atkin [4] who suggested a method of determining the expected number of points on an elliptic curve, by using complex multiplication. It now runs under the generic name ECPP (Elliptic Curve Primality Proving) and was first implemented in 1989 and continuously improved since then, by F. Morain [32].

The algorithms we present in this paper build up upon the idea of Atkin on the one hand, on extending the use of Galois rings to the context of elliptic curve primality proving and, finally, on a novel concept of *dual elliptic primes*. These are loose relatives of *twin primes* in imaginary quadratic extensions and allow to combine the worlds of CPP and ECPP in a new algorithm that we call CIDE. The fundamental gain of CIDE consists in eliminating the alternative (1) in CPP, thus yielding a random polynomial algorithm, which is practically an improvement

of both CPP and ECPP. We note that the computation Jacobi sums, which was an other superpolynomial step in CPP, can be solved in random polynomial time thanks to the novel algorithm of Ajtai et. al. [3]; in practice, the computation of Jacobi sums can be solved in very short time using their arithmetic properties and a PARI program for finding generators of principal ideals. Herewith CIDE is faster by a factor of $\log(n)$ then either version of ECPP; i.e. the [18], which is slower but has a proof of random polynomial run time for *almost all* inputs, or FastECPP [36], which runs de facto in time $O\left((\log(n)^{4+\varepsilon}\right)$, but the run time proof uses some heuristics. Unsurprisingly, the same kind of proofs can be provided for the two versions of CIDE: this is due to the fact that the first step of finding a pair of dual elliptic pseudoprimes requires running one round of some version of ECPP.

The structure of the paper is the following. In the next section we give some general definitions and facts related to elliptic curves over finite fields, complex multiplication and ECPP. In the third section we develop a theory of elliptic extensions of galois rings, which is a natural analog of cyclotomic extensions used in CPP [28]. Section four brings the definition of dual elliptic primes and their pseudoprime counterparts and the basic properties of pseudoprimes which are going to be exploited algorithmically in the subsequent section. Finally, section six gives run time analysis and implementation data and in section seven we draw some brief conclusions.

2. Elliptic curves and related pseudoprimes

If $\mathbb{K}$ is some field, the equation $Y^2 \equiv X^3 + AX + B$, with $A, B; X, Y \in \mathbb{K}$ and the discriminant $\Delta = 4A^3 + 27B^2 \neq 0$, defines an elliptic curve over $\mathbb{K}$. We denote it by

$$\mathcal{E}_{\mathbb{K}}(A,B) = \{\ (X,Y) \in \mathbb{K}^2 : Y^2 = X^3 + AX + B\ \}, \tag{3}$$

or simply $\mathcal{E}$ when there is no ambiguity. The elements $P = (X,Y) \in \mathcal{E}$ are *points* and the curve is endowed with an addition law, $R = P \oplus Q$ defined by

$$\begin{aligned} \lambda &= \frac{Q_y - P_y}{Q_x - P_x}, \quad \text{for} \quad P \neq Q, \\ \lambda &= \frac{3P_x^2 + a}{2P_y}, \quad \text{for} \quad P = Q, \\ R_x &= \lambda^2 - (P_x + Q_x), \quad R_y = \lambda R_x + (P_y - \lambda P_x). \end{aligned} \tag{4}$$

We let

$$\mu(P,Q) = \begin{cases} Q_x - P_x & \text{if} P \neq Q, \\ 2P_y & \text{otehrwise} \end{cases}.$$

The neutral element is the *point at infinity* $\mathfrak{O}$ and $P \oplus Q = \mathfrak{O}$ iff $\mu(P,Q) = 0$; the inverse of $P = (X,Y)$ is $-P = (X,-Y)$. This makes $\mathcal{E}$ into an abelian group - see also [41], §2.2. The k - fold addition of a point with itself is written $[k]P$ and can be expressed by explicite polynomials over $\mathbb{K}$:

$$[k]P = \left(\frac{\phi_n(P_x)}{\psi_n^2(P_x)}, P_y\frac{\omega_n(P_x)}{\psi_n^3(P_x)}\right), \quad \text{with} \quad \phi_n, \psi_n, \omega_n \in \mathbb{Z}[A,B], \tag{5}$$

see [41], Theorem 3.6, where the Y coordinates are given by some bivariate polynomials. These can be reduced to mono-variate ones as above.

The k - torsion of $\mathcal{E}_{\mathbb{K}}(A,B)$ is the set

$$\mathcal{E}_{\mathbb{K}}(A,B)[k] = \left\{ P \in \mathcal{E}_{\overline{\mathbb{K}}}(A,B) : [k]P = \mathfrak{O} \right\}.$$

Note that the torsion if defined over the algebraic closure; if the characteristic is 0 or coprime to k, then $\mathcal{E}_{\mathbb{K}}(A,B)[k] \cong \mathbb{Z}/(k\cdot\mathbb{Z}) \oplus \mathbb{Z}/(k\cdot\mathbb{Z})$, e.g. [41], Chapter 3. Furthermore, the torsion is related to the zeroes of $\psi_k(X)$ by

$$\mathcal{E}_{\mathbb{K}}(A,B)[k] = \left\{ P \in \mathcal{E}_{\overline{\mathbb{K}}}(A,B) \ : \ \psi_k(P_x) = 0. \right\} \tag{6}$$

In algorithmic applications, the field $\mathbb{K}$ is a finite field. Here it is mostly a prime field $\mathbb{F}_p$, with p a rational prime and we write $\mathcal{E}_{\mathbb{F}_p} = \mathcal{E}_p$. In this case, the size of the group is bounded by the Hasse interval

$$m = |\mathcal{E}_p| \in \left((\sqrt{p}-1)^2, \sqrt{p}+1)^2 \right).$$

It is useful to consider the addition law of elliptic curves also over rings $\mathbb{Z}/(n\cdot\mathbb{Z})$, with n a rational integer, which needs not be a prime. In such cases the addition law is not everywhere defined, but it turns out that exactly the points P, Q for which $P \oplus Q$ is not defined are of great algorithmic use. The application of this generalization are found in factoring and primality testing. Since the conditions which are given in fields by $T \neq 0$ – e.g. for $T = \mu(P., Q)$ or $T = \Delta$ – are replaced by GCD computations and the requirement that $T \in (\mathbb{Z}/n\cdot\mathbb{Z})^*$, whenever such a condition is not met, a possible non trivial factor of n is found. Thus the fact that addition is not defined in such a case turns out to be an advantage rather then a nuissance, since finding non trivial factors achieves the goal of the algorithm.

Formally, for a given $n \in \mathbb{N}_{>1}$ one lets

$$\begin{aligned} \mathcal{E}_n(A,B) &= \{ \ (X,Y) \in (\mathbb{Z}/(n\cdot\mathbb{Z}))^2 : Y^2 = f(X) \ \}, \quad \text{with} \\ f(X) &= X^3 + AX + B \end{aligned} \tag{7}$$

where $A, B \in \mathbb{Z}/(n\cdot\mathbb{Z})$ are such that $4A^3 + 27B^2 \in (\mathbb{Z}/n\cdot\mathbb{Z})^*$. Addition of two points is defined by (4) *whenever* $\mu(P,Q) \in (\mathbb{Z}/n\cdot\mathbb{Z})^*$. Certainly, the pair $(\mathcal{E}_n, \oplus)$ does not define a curve in the sense of algebraic geometry and is not even a group. We may however and shall refer to the set of points $\mathcal{E}_n(A,B)$ as the elliptic curve with parameters A, B over $\mathbb{Z}/(n\cdot\mathbb{Z})$ and use the partial addition on this curve.

In primality testing we have the usual ambiguity consisting in the fact that the curves $\mathcal{E}_n$ which we use are defined in the sense of (7); if a test for n completes successfully, they turn out to be proper curves in the sense of algebraic geometry, defined over the field $\mathbb{F}_n$. Otherwise, non trivial factors of n or other contradictions to the hypothesis that n is a prime may be encountered in the process of a test.

Due to (5), the k - fold addition can be uniquely defined for any $P \in \mathcal{E}_n(A,B)$ such that $\psi_k(P_x) \in (\mathbb{Z}/n\cdot\mathbb{Z})^*$; it does not depend on particular addition chains for k. Note that since $A, B \in \mathbb{Z}/(n\cdot\mathbb{Z})$ and $\psi_k \in \mathbb{Z}[A,B]$, the division polynomial $\psi_k(X) \in \mathbb{Z}/(n\cdot\mathbb{Z})[X]$. Let the k - torsion in this case be

$$\mathcal{E}_n(A,B)[k] = \{ P \in \mathcal{E}_n(A,B) : (\psi_k(P_x), n) \neq 1 \}.$$

We say that a torsion point $P \in \mathcal{E}_n(A,B)$ is proper, if $(\psi_k(P_x), n) = n$; for an improper k - torsion point, an algorithm using k - multiplication on $\mathcal{E}_n(A,B)$ would end by featuring a non trivial divisor of n.

Note that unlike the field case, we have only defined torsion points of $\mathcal{E}_n(A,B)$ which lay in $(\mathbb{Z}/(n\cdot\mathbb{Z}))^2$. For the general case, we need a substitute for the algebraic closure of a field. For this we define the following formal algebras:

Definition 1. *Let $\rho_k(X)|\psi_k(X)$ be a polynomial such that $(\rho_k(X), \psi_i(X)) = 1$ for $i < k$. We define a* ***k-torsion algebra*** $\mathbf{R}$ *and the two points k-torsion algebra* $\mathbf{R'}$ *by:*

$$\begin{aligned} \mathbf{R} &= \mathbb{Z}/(n\cdot\mathbb{Z})[X]/(\rho_k(X)) \quad \text{and } \Theta = X \bmod \rho_k(X) \in \mathbf{R}, \\ \mathbf{R'} &= \mathbf{R}[Y]/\left(Y^2 - f(\Theta)\right), \quad \Omega = Y \bmod \left(Y^2 - f(\Theta)\right) \in \mathbf{R'}. \end{aligned} \tag{8}$$

In an two points torsion algebra $\mathbf{R}'$, the pair $P = (\Theta, \Omega) \in \mathbf{R'}^2$ verifies by construction the equation of $\mathcal{E}_n(A, B) : Y^2 = f(X)$.

We claim that the iterated addition $[i]P$ is defined for P and each $i < k$. Indeed, if this were not the case for some $i < k$, there is a prime $p|n$ and a maximal ideal $\mathfrak{P} \subset \mathbf{R}'$ containing p, such that $[i]P \bmod \mathfrak{P} = \mathfrak{O}_p$, the point at infinity of the curve $\mathcal{E}_{\overline{\mathbb{F}_p}}(A \bmod p, B \bmod p)$. This contradicts the premise $(\rho_k(X), \psi_i(X)) = 1$, thus confirming the claim. It follows that the points $[i]P \in \mathbf{R'}^2$ are k - torsion points in the two points algebra [1].

There is a unique monic polynomial $g_i(X) \in \mathbb{Z}/(n\cdot\mathbb{Z})[X]$ of degree $< \deg(\psi_k(X))$, such that $\psi_i^2(X) \cdot g_i(X) \equiv \phi_i(X) \bmod \psi_k(X)$. Then $g_i(\Theta) = ([i]P)_x$, by (5), since $\psi_k(\Theta) = 0$. We have thus:

$$g_i(\Theta) = ([i]P)_x, \quad \text{with} \quad P = (\Theta, \Omega) \in \mathbf{R'}^2. \tag{9}$$

A *size* $s\left(\mathcal{E}_n\right)$ will be the result of some algorithm for computing the number of elements of an elliptic curve in the case when n is prime. The size may depend upon the algorithm with which it is computed. Two approaches are known: the variants of Schoof's algorithm [38] and the complex multiplication approach of Atkin [4].

We can herewith extend some notions of pseudoprimality to elliptic curves:

Definition 2. *Let n be an integer and $\mathcal{E}_n(A, B)$ a curve with size m. We say that n is elliptic Fermat pseudoprime with respect to this curve, if there is a point $P \in \mathcal{E}_n(A, B) \in \mathcal{E}_n(A, B)[m]$.*

Furthermore, if $q|m$ is an integer, we say that n passes an elliptic Lucas - Lehmer test of order q (with respect to $\mathcal{E}_n(A, B)$), if there is a point $P \in \mathcal{E}_n(A, B)[q]$.

The test of Goldwasser and Kilian [18], which is the precursor of ECPP, can herewith be stated as follows: given n, find a curve $\mathcal{E}_n(A, B)$ with a size m divisible by a probable prime $q > (p^{1/4} + 1)^2$ and show that n passes a Lucas - Lehmer test for q. If q is an actual prime, then the test implies that n is also one. So one iterates the procedure for q, obtaining a descending chain which reaches probable primes of polynomial size in $O(\log(n))$ steps. In [18] sizes are estimated using the algorithm of Schoof. Even in the much faster version of these days [9], this would still yield an impractical algorithm. It does have the advantage of a provable run time analysis.

If the field $\mathbb{K} = \mathbb{F}_q$ is a finite field of characteristic p, then the Frobenius map $\Phi_q : X \mapsto X^q$ is an endomorphism of $\mathcal{E}_{\overline{\mathbb{F}_q}}(A, B)$ and verifies a quadratic equation:

$$\Phi_q^2 - t\Phi_q + q = 0 \tag{10}$$

in $\text{End}\left(\mathcal{E}_{\overline{\mathbb{F}_q}}(A, B)\right)$, as shown for instance in [39], p. 135. The number t is related to the size of the group $\mathcal{E}$ over $\mathbb{F}_q$ by $|\mathcal{E}_q| = q + 1 - t$. In particular, if $q = p = \pi \cdot \overline{\pi}$,

[1] We are not interested here in the problem of constructing algebras which contain, like in the field case, two linear independent torsion points.

for $\pi\mathcal{O} \subset \mathbb{K}$, the "CM field" of $\mathcal{E}$ (see below), then $t = \mathbf{Tr}(\pi)$, [13] Chapter 14, in particular Theorem 14.6 .

The Frobenius acts as a linear map on $\mathcal{E}_q(A,B)[k]$. If $k = \ell$ is a prime, $\mathcal{E}[\ell]$ is a vector space and there is a matrix $M_\ell(\Phi_q) \in \mathrm{GL}_2(\mathbb{F}_\ell)$ associated to the Frobenius modulo ℓ. The reduced equation (10) modulo ℓ is also the characteristic polynomial of $M_\ell(\Phi_q)$.

If $\delta = t^2 - 4q$ is a quadratic residue over $\mathbb{F}_\ell$: $\left(\frac{\delta}{\ell}\right) = 1$, then the equation (10) has two distinct roots $\bmod \ell$, which are the *eigenvalues* $\lambda_{1,2} \in \mathbb{F}_\ell^\times$ of the Frobenius. Accordingly, there are points $P_{1,2} \in \mathcal{E}_q(A,B)[\ell]$ such that

$$\Phi_q(P_i) = [\lambda_i]P_i, \quad i = 1, 2.$$

In the context of algorithms for *counting points on elliptic curves* [38], the primes with $\left(\frac{\delta}{\ell}\right) = 1$ are often referred as *Elkies primes*, while all other primes are *Atkin* primes. In this case, to each eigenvalue there corresponds an *eigenpolynomial* defined by

$$F_i(X) = \prod_{k=1}^{(\ell-1)/2} \left(X - \left([k]P_i\right)_x\right) \in \mathbb{F}_q[X], \quad i = 1, 2. \tag{11}$$

Here $\left([k]P_i\right)_x$ is the x - coordinate of the point $[k]P_i$. Various algorithms have been developed for the fast computation of the eigenpolynomials, without prior knowledge of the eigenpoints or eigenvalues; see for instance [9] for a recent survey.

2.1. **Complex Multiplication and Atkin's approach to ECPP.** We recall some facts about complex multiplication and refer to [13], Chapter 14 and [39], Chapter V, for more in depth treatment.

Fact 1. *Let p be a prime and $\mathcal{E}_p(A,B)$ be an ordinary elliptic curve*[2]*. Then there is a quadratic imaginary field $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ and an order $\mathcal{O} \subset \mathbb{K}$ such that:*

1. *The endomorphism ring of $\mathcal{E}_p(A,B)$ is isomorphic to $\mathcal{O}$.*
2. *There is a $\pi \in \mathcal{O}$ such that $p = \pi \cdot \overline{\pi}$ and the number of points*

$$|\mathcal{E}_p(A,B)| = \mathbf{N}(\pi \pm 1), \tag{12}$$

   the sign being defined only up to twists.
3. *If $H_{\mathcal{O}}(X) \in \mathbb{Z}[X]$ is a polynomial which generates the ring class field $\mathbb{H}$ of $\mathcal{O}$, i.e. $\mathbb{H} = \mathbb{K}[X]/\left(H_{\mathcal{O}}(X)\right)$, then $H_{\mathcal{O}}(X)$ splits completely modulo p.*
4. *There is a zero $j_0 \in \mathbb{H}$ of the polynomial $H_{\mathcal{O}}(X)$ and an elliptic curve $\mathcal{E}_{\mathbb{H}}(a,b)$ defined over $\mathbb{H}$ such that:*
   a) *The j -invariant of $\mathcal{E}_{\mathbb{H}}(a,b)$ is j_0, of $r(j_0)$ with $r(X) \in \mathbb{Q}(X)$.*
   b) *Its endomorphism ring is isomorphic to $\mathcal{O}$ and*
   c) *The curve has good reduction at a prime $\wp \subset \mathcal{O}(\mathbb{H})$ above (p).*
   d) *The reduction is $\mathcal{E}_p(A,B)$ and it is a direct consequence of CM, that $\mathcal{E}_p(A,B)$ is ordinary.*

   Under these circumstances, the curve $\mathcal{E}_{\mathbb{H}}(a,b)$ is unique and is called the Deuring lift of $\mathcal{E}_p(A,B)$.

In $\mathcal{O}$, the prime p splits in principal ideals in $\mathcal{O}$ if and only if 3. holds - see e.g. [13] *Theorem 9.2 for the case when $\mathcal{O}$ is the maximal order. In particular:*

$$p = \pi \cdot \overline{\pi} \quad \textit{with} \quad \pi \in \mathcal{O} \quad \Leftrightarrow \quad \exists\, x \in \mathbb{F}_p : \; H_{\mathcal{O}}(x) = 0. \tag{13}$$

[2]A curve is ordinary if it is regular and not supersingular, [41], p. 75

Thus the endomorphism ring associates an order in an imaginary quadratic field to an ordinary elliptic curve over a finite field - the association being actually an isomorphism of rings. Non-isomorphic curves can be associated to one and the same order. This fact allows to construct curves over a finite field $\mathbb{F}_p$ which have a known endomorphism ring and thus the size may be derived directly from (12). The algorithm involves the construction of polynomials $H_{\mathcal{O}}(X)$ for various orders of small discriminant until one is found which splits completely modulo p. The methods for computing $H_{\mathcal{O}}(X)$ have been subject of investigation for over a decade; see [33] for an in depth treatment and [9] for current improvements. The advantage of this approach, is that curves with known size can be computed faster then by using the best versions of Schoof's algorithm for computing the size of a given curve. Thus although this approach is not used for finding the size of a given curve, it is sufficient for some application where it suffices to know *some* curve together with its number of points.

The idea of Atkin was to produce similar associations for curves $\mathcal{E}_n(A,B)$, with n not necessarily prime, and to estimate their size using the equation in (12). In order to produce such an association, one uses algorithms for finite fields. The construction may thus stop with a contradiction to the hypothesis that n is prime. Otherwise it is expected to produce an order $\mathcal{O} \subset \mathbb{Q}[\sqrt{-d}]$ in which n factors in principal ideals $n = \nu \cdot \overline{\nu} : \ \nu \in \mathcal{O}$ and such that $H_{\mathcal{O}}(X)$ has a linear factor in $\mathbb{Z}/(n \cdot \mathbb{Z})$. Furthermore, it produces a curve $\mathcal{E}_n(A,B)$ with *Atkin size* $m = \mathbf{N}(\nu \pm 1)$ as suggested by (12). Several discriminants d are tried, until it is found by trial factorization that m is divisible by a large pseudoprime q. Finally, a point $P \in \mathcal{E}_n(A,B)$ is sought, such that $\psi_q(P_x) \notin (\mathbb{Z}/n \cdot \mathbb{Z})^*$. If P is not a proper $q-$th torsion point, a non trivial factor of n is found and the algorithm terminates. Otherwise, if q is in fact prime, then so must n be, by the Lucas - Lehmer argument. This leads to an iterative primality proof, like in the case of Goldwasser and Kilian, but with a faster estimation of the size. However, since the discriminants d must have polynomial size, the curves taken into consideration are not random. Unlike the case of [18], the fact that one can find in polynomial time a discriminant such that the above conditions hold is supported by heuristic arguments. Such arguments are given in [17].

We introduce the following notion of pseudoprimes, related to the above algorithm:

Definition 3. *Let n be an integer and $\mathcal{E}_n(A,B)$ be an elliptic curve (with partial addition), $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ be a quadratic imaginary field and $\mathcal{O} \subset \mathbb{K}$ some order. We say that $(\mathcal{E}_n(A,B), \mathcal{O})$ are* associated *if the following conditions are fulfilled:*

1. *The integer n is square free, there is a $\nu \in \mathcal{O}$ such that $n = \nu \cdot \overline{\nu}$, and*

$$(n, \nu + \overline{\nu}) = 1. \tag{14}$$

2. *There is a polynomial $H_{\mathcal{O}}(X) \in \mathbb{Z}[X]$, which generates the ring class field $\mathbb{H}$ of $\mathcal{O}$, i.e. $\mathbb{H} = \mathbb{K}[X]/\left(H_{\mathcal{O}}(X)\right)$ and which has a zero $\jmath_0 \in (\mathbb{Z}/n \cdot \mathbb{Z})^*$. Furthermore, the j - invariant of $\mathcal{E}_n(A,B)$ is a rational function in $\jmath_0$.*

Remark 1. *We refer the reader to* [4, 15, 16] *for details on techniques for choosing the polynomial $H_{\mathcal{O}}$. It should be mentioned that the* modular equation *is a theoretical alternative for the polynomial $H_{\mathcal{O}}(X)$, and it has the j - invariants as*

zeroes; however, from a computational point of view, the modular equation is impractical, having very large coefficients, so one constructs alternative polynomials which generate the same field.

Based on the associations of curves and orders, one defines Atkin pseudoprimes as follows:

Definition 4. *We say that n is **Atkin pseudoprime**, if*

- *There is a curve $\mathcal{E}_n(A,B)$ associated to an order $\mathcal{O} \subset \mathbb{K} = \mathbb{Q}[\sqrt{-d}]$ according to the above definition.*
- *The Atkin size of $\mathcal{E}_n(A,B)$ is $m = \mathbf{N}(\nu \pm 1)$ and is divisible by a strong pseudoprime $q > \left(n^{1/4}+1\right)^2$.*
- *There is a proper q - torsion point $P \in \mathcal{E}_n(A,B)$*[3]

The pseudoprime n is thus given by the values

$$(n; (\mathcal{E}_n(A,B), \mathcal{O}); P, q)\,.$$

In all versions of the ECPP test, one seeks a random curve whose size is divisible by some large pseudoprime q. When the parameters $A, B \in \mathbb{Z}/(n\cdot\mathbb{Z})$ are chosen uniformly random. In this case, if n is a prime, it is known that the sizes of the curves are close to uniform distributed in the Hasse interval [14], Theorem 7.3.2. This fact is useful for the run time analysis of the Goldwasser - Kilian test.

Atkin's test builds descending sequences of Atkin pseudoprimes $n, q, \ldots$, until pseudoprimes of polynomial size are reached. The discriminant $-d$ of the field $\mathbb{K}$ must be polynomial in size, which is an important restriction for the choice of $\mathcal{O}$. For prime n, the density of the curves with CM in fields with polynomial discriminant is exponentially small. Thus Theorem 7.3.2 does not hold and there is thus no *proof* for the fact that ECPP terminates in polynomial time even on *almost* all inputs.

We note the following consequence of condition 2.:

Lemma 1. *Suppose that $n > 2$ is an integer for which there exists an association $(\mathcal{E}_n(A,B), \mathcal{O})$ according to Definition 3 and let $p|n$ be a rational prime. Then $\mathcal{E}_p(\overline{A}, \overline{B})$ with $\overline{A} = A \text{ rem } p, \overline{B} = B \text{ rem } p$ is an elliptic curve over the field $\mathbb{F}_p$ with CM in $\mathcal{O}$ and p splits in principal ideals in this order, say $p = \pi\cdot\overline{\pi}$.*

Proof. The curve $\mathcal{E}_p(\overline{A}, \overline{B})$ is defined by reduction modulo p. The polynomial $H_{\mathcal{O}}(X)$ has a root $\jmath_0 \in \mathbb{Z}/(n\cdot\mathbb{Z})$ and thus $\overline{\jmath}_0 = \jmath_0 \bmod p$ is a root thereof in $\mathbb{F}_p$. The j invariant will then be a rational function of this value. Then (13) implies that $p = \pi\cdot\overline{\pi}$. □

3. Gauss sums and CPP

The Jacobi sum test [1, 21], which is the initial version of CPP is based on the use of Gauss and Jacobi sums. Over some field $\mathbb{K}$, these are classical character sums, see e.g. [20], Chapter 8. In primality testing however, the images of the characters are taken over some ring $\mathbb{Z}/(n\cdot\mathbb{Z})$ which need not be a field. We need thus a dedicated context of *cyclotomic extensions of rings* for the definition of these sums.

[3] Since $q|m$, a q torsion point should be found in the curve over $\mathbb{Z}/(n\cdot\mathbb{Z})$, if n is prime, so the condition is consistent.

Since their definition by Lenstra [23], cyclotomic extensions have undergone various modifications [8, 26, 27, 24] until the recent "pseudo-fields" [24, 25]. We shall follow use here definitions given in [5, 27]. Proofs of the facts we shall need are in [26, 27].

Let $n \in \mathbb{N}$ be an integer and consider rings of characteristic n, more precisely finite Abelian ring extensions $\mathbf{R} \supset \mathbb{Z}/(n\cdot\mathbb{Z})$. Galois extensions [27] are simple algebraic extensions of the form $\mathbf{R} = \mathbb{Z}/(n\cdot\mathbb{Z})[T]/(f(T))$ endowed with automorphisms which fix $\mathbb{Z}/(n\cdot\mathbb{Z})$. We are interested in the *simple Frobenius extensions* defined by:

Definition 5. *Let $\mathbf{R}$ be a finite commutative ring of characteristic n and $\Psi(X) \in \mathbf{R}[X]$ a monic polynomial. We say that the ring extension $\mathbf{R} = \mathbb{Z}/(n\cdot\mathbb{Z})[X]/(\Psi(X))$ is simple Frobenius if:*

F1. *There is a $t > 0$ such that*

$$\Psi(X) = \prod_{i=1}^{t} \left(X - \zeta^{n^i}\right), \qquad \textit{where} \quad \zeta = X + (\Psi(X)) \in \mathbf{R}.$$

F2. *Let $x_i = \zeta^{n^i} \in \mathbf{A}$. There is a $\sigma \in$ Aut $_{\mathbf{R}}/\mathbb{Z}/(n\cdot\mathbb{Z})$ acting like a cyclic permutation on $S = \{x_1, x_2, \ldots, x_t\}$.*

Let $s \in \mathbb{Z}_{>1}$ and $\Phi_s(X) in \mathbb{Z}[X]$ be the $s-$th cyclotomic polynomial. If $\Psi(X) \in \mathbb{Z}/(n\cdot\mathbb{Z})[X]$ is a polynomial with $\Phi_s(X) \equiv 0 \bmod (n, \Psi(X))$ and the extension $\mathbf{R} = \mathbb{Z}/(n\cdot\mathbb{Z})/(\Psi(X))$ is simple Frobenius, we say that $(\mathbf{R}, \zeta, \sigma)$ is an $s-$th ***cyclotomic extension*** *of $\mathbb{Z}/(n\cdot\mathbb{Z})$.*

In general, if $\mathbf{R} \supset \mathbb{Z}/(n\cdot\mathbb{Z})$ is an algebra and $\zeta \in \mathbf{A}$ is such that $\overline{\Phi}_s(\zeta) = 0$, with $\overline{\Phi}_s(X) = \Phi_s(X) \bmod n$, then we say that ζ is a ***primitive*** *$s-$th root of unity modulo n.*

Remark 2. *The reader may regard a cyclotomic extension $\mathbf{R}$ as an extension of the ring $\mathbb{Z}/(n\cdot\mathbb{Z})$ which contains a primitive $s-$th root of unity ζ and on which an automorphism acts, that fixes $\mathbb{Z}/(n\cdot\mathbb{Z})$. One can prove - without knowing that n is prime - sufficient properties about $\mathbf{R}$ in order to be allowed to work in the extension as if it was a finite field and n were a prime – this behavior justifies the name of pseudo-fields recently employed by Lenstra.*

The pairs (n, s) for which cyclotomic extensions exist are exceptional. The existence of such pairs is a strong property of n with respect to s, that often qualifies n to behave like a prime. The following fact reflects this claim: an $s-$th cyclotomic extension of $\mathbb{Z}/(n\cdot\mathbb{Z})$ exists if and only if

$$r \in \langle n \bmod s \rangle \quad \text{for all} \quad r \mid n \ . \tag{15}$$

Let p be an odd prime and $k(p) = v_p\left(n^{p-1} - 1\right)$, with v_p the p-adic valuation. If it exists, a $p-$th cyclotomic extension of $\mathbb{Z}/(n\cdot\mathbb{Z})$ may contain also a $p^{k(p)}-$th primitive root of unity; this is in fact true if n is a prime. This leads to the following

Definition 6. *Let p be a prime. The* saturation exponent *of p is:*

$$k(p) \quad = \quad \begin{cases} v_2(n^2-1) & \textit{if } p = 2 \textit{ and } n = -1 \bmod 4 \\ \\ v_p\left(n^{p-1} - 1\right) & \textit{otherwise} \end{cases} \tag{16}$$

Let $m = \prod_i p_i^{e(i)} \in \mathbb{N}$ be the prime factorization of an integer. The (n-)saturated order above m *is:*

$$\overline{m} = \prod_i p_i^{\max(e(i),k(p_i))} \quad .$$

An $m-$th *cyclotomic extension* $(\mathbf{R}, \sigma, \zeta)$ *is called* saturated *if* $m \geq \overline{m}$ *and* subsaturated *otherwise. If* $e(i) = k(p_i)$ *for all* $p_i \mid m$*, the extension is* minimal saturated.

Saturated extensions are characterized by the following property:

Fact 2. *If* $(\mathbf{R}, \sigma, \zeta)$ *is a saturated* $m-$th *extension and* $m' \mid m^h$ *for some* $h > 0$ *(i.e.* m' *is built up from primes dividing* m*), then* $\mathbf{R}[X]/(X^{m'} - \zeta)$ *is an* $m \cdot m'-$th *cyclotomic extension.*

If $(\mathbf{R}, \sigma, \zeta), (\mathbf{R'}, \sigma', \zeta')$ *are saturated* $m-$th *and* $m'-$th *extensions for* $(m, m') = 1$*, then* $(\mathbf{R} \times \mathbf{R}', \sigma \circ \sigma', \zeta \cdot \zeta')$ *is a saturated* $mm'-$th *extension, for the natural lifts of* σ, σ' *to* $\mathbf{R} \times \mathbf{R}'$*.*

The use of saturated extensions in primality testing is given by the following

Lemma 2 (Cohen and Lenstra, [11])**.** *Suppose that* p *is a prime with* $(p, n) = 1$*, for which a saturated* $p-$th *cyclotomic extensions of* $\mathbb{Z}/(n \cdot \mathbb{Z})$ *exists. Then for any* $r|n$ *there is a* p*-adic integer* $l_p(r)$ *and, for* $p > 2$*, a number* $u_p(r) \in \mathbb{Z}/((p-1) \cdot \mathbb{Z})$*, such that:*

$$\begin{aligned} r &= n^{u_p(r)} \mod p \quad \textit{and} \\ r^{p-1} &= (n^{p-1})^{l_p(r)} \in \{1 + p \cdot \mathbb{Z}_p\} \quad \textit{if} \quad p > 2, \\ r &= n^{l_p(r)} \in \{1 + 2 \cdot \mathbb{Z}_2\} \quad \textit{if} \quad p = 2. \end{aligned} \tag{17}$$

Proof. Using (15), the hypothesis implies that $r \in < n \mod p^k >$ for all $k \geq 1$ which implies (17). □

Gauss and Jacobi sums over $\mathbb{Z}/(n \cdot \mathbb{Z})$ will be defined by means of characters over saturated extensions. Let p, q be two rational primes which do not divide n, let $k > 0$ and $(\mathbf{R}, \zeta, \sigma)$ be a saturated p^k-th extension which additionally contains a primitive $q-$th root of unity ξ; the ring $\mathbf{R}$ need not be minimal with these properties. Let χ be a multiplicative character $\chi : (\mathbb{Z}/q \cdot \mathbb{Z})^* \to < \zeta >$ of conductor q and order $d|p^k$. If $d = 1$, χ is the trivial character 1. The (cyclotomic) Gauss sum of χ with respect to ξ is

$$\tau(\chi) = \sum_{x \in (\mathbb{Z}/q \cdot \mathbb{Z})^*} \chi(x) \xi^x.$$

It can be shown that $\tau(\chi) \in \mathbf{R}^\times$, since $\tau(\chi) \cdot \tau(\chi^{-1}) = \chi(-1) \cdot q$. For $a, b \in \mathbb{Z}$ such that $\chi^a, \chi^b, \chi^{a+b} \neq 1$, the Jacobi sum

$$j(\chi^a, \chi^b) = \sum_{x=2}^{q-1} \chi^a(x) \chi^b(1-x) = \frac{\tau(\chi^a) \cdot \tau(\chi^b)}{\tau(\chi^{a+b})}.$$

The *multiple Jacobi-Sums* $J_\nu(\chi)$ are defined by:

$$\begin{aligned} J_1 &= 1 \\ J_{\nu+1} &= J_\nu \cdot j(\chi, \chi^\nu), \quad \text{for } \nu = 1, 2, \ldots, d-2 \\ J_d &= \chi(-1) \cdot m \cdot J_{d-1} \end{aligned} \tag{18}$$

It is easy to verify by induction that:

$$J_\nu = \frac{\tau(\chi)^\nu}{\tau(\chi^\nu)}, \quad \text{for } \nu = 1, 2, \ldots, d, \text{ where } \quad \chi^d = 1. \tag{19}$$

Let $s = \prod_{q \in Q} q$ be a product of primes from the set Q such that there is a $t = \prod_{p^k \in P} p^k$ with P a set of prime powers and for all $q \in Q,\ q-1|t$. Let $\mathbf{R}$ be the product of saturated p^k-th cyclotomic extensions and $C = \left\{\chi_{p^k,q} \ : \ p^k \in P, q \in Q\right\}$ be a set of characters of conductor q and order p^k with images in $\mathbf{R}$. If $n = b(p^k) \cdot p^k + r(p^k)$ is the Euclidian division of n by each p^k, it can be shown [8, 26, 28] that a cyclotomic $s-$th extension of $\mathbb{Z}/(n \cdot \mathbb{Z})$ exists if

$$J_{p^k}^{b(p^k)}(\chi_{p^k,q}) \cdot J_{r(p^k)}(\chi_{p^k,q}) \in < \zeta_{p^k} >, \quad \text{for each} \quad \chi \in C. \tag{20}$$

Verifying these relations is the main stage of the CPP test.

Remark 3. *Due to an analytic number theoretical Theorem of Pracher, Odlyzko and Pomerance, one knows that two parameters s, t can be chosen, such that $s > \sqrt{n}$ and $t = O\left(\log(n)^{\log\log\log(n)}\right)$, while $s|(n^t - 1)$ for any n. The complexity of CPP is polynomial in t; both the number of prime powers dividing t and their size are upper bounded by*

$$B = O(\log\log(n)), \quad \omega(t) < B \quad \textit{and} \quad p^k||t \Rightarrow p^k < B. \tag{21}$$

We shall use an auxiliary construction involving *dual elliptic primes* in order to show that if n passes the tests (20) together with some additional conditions - which are more involved to formulate, but can be verified faster then (20) - then either n is prime, or it has a prime factor r with $l_{p^k}(r) = 1$ for all $p^k \in P$.

The constructions involve elliptic Gauss and Jacobi sums, which we shall introduce below. We first define the simples analogue of cyclotomic extensions for elliptic curves.

Definition 7. *Let $n > 2$ be an integer and $\ell \nmid n$ be an odd prime. Let $\mathcal{E}_n(A, B)$ be an elliptic curve and $\psi_\ell(X)$ be the $\ell-$th division polynomial of the curve. Suppose that $F(X) \in \mathbb{Z}/(n \cdot \mathbb{Z})[X]$ is such that*

1. *$F(X)|\psi_\ell(X)$.*
2. *If $\mathbf{E} = \mathbb{Z}/(n \cdot \mathbb{Z})[X]/(F(X))$ and $\Theta = X \bmod F(X) \in \mathbf{R}$, then*

$$F(T) = \prod_{i=1}^{(\ell-1)/2} (T - g_i(\Theta)),$$

where $g_i(X)$ are the multiplication polynomials defined in (9). In particular the elementary symmetric polynomials of Θ lay in $\mathbb{Z}/(n \cdot \mathbb{Z})$.

*Then $F(X)$ is called an **Elkies factor** of $\psi_\ell(X)$ over $\mathbb{Z}/(n \cdot \mathbb{Z})$ and $\mathbf{E}$ is an **Elkies ring**. Additionally, we let*

$$\mathbf{E'} = \mathbf{E}[Y]/\left(Y^2 - f(\Theta)\right) \quad \textit{and} \quad \Omega = Y \bmod (f(\Theta) \in \mathbf{E'}$$

be the two coordinates Elkies ring.

Let $(\mathbf{R}, \zeta, \sigma)$ be a saturated $\ell-1-$th cyclotomic extension and $\chi : (\mathbb{Z}/\ell \cdot \mathbb{Z})^* \to \mathbf{R}$ be a multiplicative character of odd order. We define Gauss sums in Elkies rings

by:

$$\tau_e(\chi) = \sum_{i=1}^{\ell-1} \chi(x) g_x(\Theta)$$

In the case when the order of χ is even and $\chi(-1) = -1$, the sums above are vanishing due to the parity of P_x. One uses the Y - coordinates in the two coordinates Elkies ring, and some related multiplication polynomials. The formal definition based on repeated addition of $P = (\Theta, \Omega)$ in $\mathbf{E}'$ is in this case:

$$\tau'_e(\chi) = \sum_{i=1}^{\ell-1} \chi(x)([x]P)_Y$$

The values of $([x]P)_Y$ can be computed using Ω and polynomials in Θ; we skip the details here and refer to [29, 30] for in depth treatment of theoretical and computational aspects of elliptic Gauss and Jacobi sums.

The Jacobi sums have no closed definition like in the cyclotomic case, so they must be deduced as quotients of Gauss sums:

$$j_e(\chi^a, \chi^b) = \frac{\tau_e(\chi^a)\tau_e(\chi^b)}{\tau_e(\chi^{a+b})} \quad \text{iff } \tau_e(\chi^{a+b}) \in \mathbf{E}^\times.$$

The case $\tau_e^{a+b}(\chi) \notin \mathbf{E}^\times$ is improbable, but cannot be excluded currently. This is best explained in the case when $n = r$ is a prime. Then $\mathcal{E}_r(A, B)$ has a Deuring lift to some curve $\mathcal{E}_{\mathbb{H}}(a, b)$. The Gauss sums of curves in characteristic 0 have been studied by R. Pinch in [37] and it was shown that along with the ramified primes dividing $\ell \cdot \Delta$, where Δ is the discriminant of the curve, some spurious and unexplained primes may appear in the factorization of the Gauss sum. Since Δ reduces to the discriminant of the curve $\mathcal{E}_r(A, B)$ which is non vanishing by definition and $\ell \neq r$, the spurious primes may be divisors of r, in which case $\tau_e(\chi) \notin \mathbf{E}^\times$. If n is not prime and $(\tau_e(\chi), n) \notin \{1, n\}$, a non trivial factor is found. We shall assume in our algorithm that the case $(\tau_e(\chi), n) = n$ is scarce. It can be avoided by changing the choice of ℓ, as we shall detail below. If ℓ is a conductor, such that $(\tau_e(\chi), n) = n$ for some character of conductor ℓ, then we say that ℓ is an *exceptional conductor* (for the curve $\mathcal{E}_n(A, B)$).

If $n = r$ is a prime, then $\Theta^r = g_\lambda(\Theta)$ for some $\lambda \in (\mathbb{Z}/\ell \cdot \mathbb{Z})^*$, an eigenvalue of the Frobenius. In that case, raising the definition of the Gauss sum to the power n yields:

$$\begin{aligned} \tau_e(\chi)^r &= \left(\sum_{i=1}^{\ell-1} \chi^r(x) g_x(\Theta^r) \right) \\ &= \sum_{i=1}^{\ell-1} \chi^r(x) g_{\lambda x}(\Theta) = \chi^{-r}(\lambda)\tau_e(\chi^r) \end{aligned}$$

and

$$\tau_e(\chi)^r / \tau_e(\chi^r) = \chi^{-r}(\lambda). \tag{22}$$

The right hand side of the equation can be computed, like in the cyclotomic case by using multiple Jacobi sums in $\mathbf{R}$.

4. Elliptic extensions of rings

In this section we generalize the notion of *cyclotomic extension of rings* to elliptic curves. We shall say that an Elkies algebra is elliptic extension of $\mathbb{Z}/(n\cdot\mathbb{Z})$, if the power n acts like a Frobenius, i.e. (22) is verified when the prime r is replaced by n. Note that this is a slightly milder condition then the one for cyclotomic extensions, since we are not interested in finding an actual factor of $F(X)$ which has degree equal to the order of n in the group $(\mathbb{Z}/\ell\cdot\mathbb{Z})^*/\{-1,1\}$, i.e. the degree of an irreducible factor of $F(X)$ in the case when n is prime.

Definition 8. *Let $m\in\mathbb{N}_{>2}$ be an elliptic Atkin pseudoprime: there is a curve $\mathcal{E}_m(A,B):Y^2=X^3+A\cdot X+B$ associated to an order $\mathcal{O}\subset\mathbb{K}=\mathbb{Q}(\sqrt{-d})$ and such that $m=\mu\cdot\overline{\mu}$ for a $\mu\in\mathcal{O}$. Let ℓ be a rational prime such that $\left(\frac{-d}{\ell}\right)=1$:*

A. *For each prime power $q||(\ell-1)$, there is a saturated $q-$th cyclotomic extension $\mathbf{R}_q\supset\mathbb{Z}/(m\cdot\mathbb{Z})$. The rings $\mathbf{R}-q$ will also be called* working extensions.
B. *There is an $\ell-$th cyclotomic extension $\mathbf{R}_\ell\supset\mathbb{Z}/(m\cdot\mathbb{Z})$ constructed by verifying (20) over the extensions $\mathbf{R}_q$.*
C. *In particular, then*

$$r\equiv n^{l_p(r)}\bmod\ell,\quad \text{for } p|q \text{ a prime and for all } \quad r|m. \tag{23}$$

Let $\psi_\ell(X)$ be the $\ell-$th division polynomial associated to $\mathcal{E}_m(A,B)$ and suppose that an Elkies factor $F(X)|\psi_\ell(X)\bmod m$ is known and $(\mathbf{E'},\Theta,\Omega)$ is the two coordinates Elkies algebra. For a prime power $q||(\ell-1)/2$ we let $\chi_q:(\mathbb{Z}/\ell\cdot\mathbb{Z})^*\to\mathbf{R}$ be a character of order q and conductor ℓ. Suppose that:

1. *For each odd q, $(\tau_e(\chi),n)=1$ and*

$$\tau_e(\chi)^n/\tau_e(\chi^n)=\eta_q^{-n}\in<\zeta>. \tag{24}$$

2. *For even q, $(\tau'_e(\chi),n)=1$ and*

$$\tau'_e(\chi)^n/\tau'_e(\chi^n)=\eta'^{-n}_q\in<\zeta>. \tag{25}$$

If the above conditions are met, we say that an $\ell-$th elliptic extension of $\mathbb{Z}/(n\cdot\mathbb{Z})$ related to $\mathbf{R}$ exists. The conditions $\chi_q(\lambda)=\eta_q$ for odd q and $\chi_q(\lambda)=\eta'_q$ for even q uniquely determine $\lambda_m\in(\mathbb{Z}/\ell\cdot\mathbb{Z})^*$. This value will be denoted as the eigenvalue of the elliptic extension $\mathbf{E}$.

The point C. of the definition is a fact following from points A. and B. and not a condition. The main fact about elliptic extensions is the following:

Theorem 2. *Let $n\in\mathbb{N}_{>2}$ be an integer and ℓ a prime not dividing n. If all the conditions for existence of an $\ell-$th elliptic extension of $\mathbb{Z}/(n\cdot\mathbb{Z})$ are fulfilled and $r|n$ is a prime, $\mathcal{E}_r(\overline{A},\overline{B})=\mathcal{E}_n(A,B)\bmod r$, then*

A. *The curve $\mathcal{E}_r(\overline{A},\overline{B})$ has CM in $\mathcal{O}$ and $\overline{F}(X)=F(X)\bmod r$ is an Elkies factor of its $\ell-$th torsion polynomial.*
B. *There is an eigenvalue $\lambda_r\in\mathbb{F}_\ell^\times$ of the Frobenius of $\mathcal{E}_r(\overline{A},\overline{B})$ such that $P^r=[\lambda_r]P$ for all points $P\in\mathcal{E}_r(\overline{A},\overline{B})[\ell]$ such that $\overline{F}(P_x)=0$.*
C. *If λ_m is the eigenvalue of the Elkies extension, p is the prime dividing q and $l_p(r)$ is defined by (17) with respect to the extension $\mathbf{R}$, then*

$$\chi_q(\lambda_r) = \chi_q(\lambda_m)^{l_p(r)}\quad\forall q. \tag{26}$$

$$\chi_q(r/\lambda_r) = \chi_q(m/\lambda_m)^{l_p(r)}\quad\forall q. \tag{27}$$

Proof. The point A. follows from Lemma 1. Point B. follows from the factorization patterns of the division polynomial, e.g. [38], Theorems 6.1, 6.2.

For proving (26), we use the fact that $\mathbf{R}$ is a cyclotomic extension and let $\sigma : \zeta \mapsto \zeta^n$ act on the identities (24). The Y - component conditions (25) are treated identically and will not be developed here.

$$\begin{aligned} \tau_e^{n^2}(\chi_q) &= (\tau_e^n(\chi_q))^n = \big(\eta_q^{-n} \cdot \sigma(\tau_e(\chi_q)\big)^n \\ &= \eta_q^{-n^2} \cdot \sigma(\eta_q^{-n}\tau_e(\chi_q^n)) = \eta_q^{-2n^2} \cdot \sigma^2(\tau_e(\chi_q)), \dots \\ \tau_e(\chi_q)^{n^k} &= \eta_q^{-kn^k}\sigma^k(\tau_e(\chi_q)). \end{aligned} \tag{28}$$

Inserting $k = \varphi(q)$ we obtain $\tau_e^{n^{\varphi(q)}-1} = \eta_q$ and for $K = p \cdot \varphi(q)$, writing $N = n^K$, we have

$$\tau_e(\chi_q)^{N-1} = 1.$$

If $r \mid n$ is a prime, by (22),

$$\tau_e(\chi_q)^r \ \equiv \ \chi_q(\lambda_r)^{-r} \cdot (\tau_e(\chi_q^r)) \bmod r \cdot \mathbf{R}.$$

Let $m \in \mathbb{N}$ be such that $m \equiv l_p(r) \mod pq$ and $m = u_p(r) \mod (p-1)$, with $u_p(r)$ and $l_p(r)$ defined by (17). Then $\sigma^m(\chi_q) = \chi^r$ and

$$v_\ell(r - n^m) \ = \ v_\ell\big(n^m \cdot (r/n^m - 1)\big) \geq v_\ell(N-1). \tag{29}$$

We let $i = m$ in (28), use $\sigma^m\big(\tau_e(\chi_q)\big) \ = \ \tau_e(\chi_q^r)$ and divide by (29). This is allowed, since $(\tau_e(\chi_q), n) = 1$ by condition 1. Thus

$$\tau_e(\chi_q)^{n^m - r} \ \equiv \ \big(\chi_q(\lambda_r) \cdot \eta_q^{-m}\big)^r \bmod r \cdot \mathbf{R}.$$

Raising this congruence to the power a, where a is the largest divisor of $(N-1)$ which is coprime to ℓ, and using the above, we get :

$$1 \ \equiv \ \big(\chi_q(\lambda_r) \cdot \eta^{-m}\big)^{r \cdot a} \bmod r \cdot \mathbf{R}.$$

Since $(ra, \ell) = 1$, we deduce that $\chi_q(r)\eta_q^{-m} \equiv 1 \bmod r\mathbf{R}$, and since $(\ell, n) = 1$ also $\chi_q(\lambda_r)\eta_q^{-m} = 1$ and $\chi_q(\lambda_r) = \eta_q^m = \eta_q^{l_p(r)}$. This holds for all primes $r \mid n$ and by multiplicativity, for all $r|n$. In particular, since $l_p(m) = 1$, it follows that $\chi_q(\lambda_m) = \eta_q$, thus recovering the definition of the eigenvalue of the elliptic extension. The proof of (26) is complete. As for (27), it follows from (26) and (23). □

The notion of elliptic extension for composites is now straight forward:

Definition 9. *Let $L = \prod_{i=1}^k \ell_i \in \mathbb{N}$ be square-free, with ℓ_i being primes. Assume that there is an $\varphi(L)-$*th *saturated working extension $\mathbf{r}_L \supset \mathbb{Z}/(m \cdot \mathbb{Z})$ and an $L-$*th *extension $\mathbf{R}_L \supset \mathbf{r}_L$.*

*Suppose also that m is Atkin pseudoprime so there is a curve $\mathcal{E}_m(A, B)$ associated to an order $\mathcal{O} \subset \mathbb{K} = \mathbb{Q}[\sqrt{-d}]$. We say that an $L-$*th *elliptic extension exists, if the conditions of Definition 8 are fulfilled for all ℓ_i in the working extension $\mathbf{r}_L$ or subextensions thereof.*

Note that relation (26) is a strengthening of the consequence $p \equiv m^k \bmod L$, usual in classical cyclotomy tests. It follows from the definition and (26) (27) that

$$\lambda_r \ \equiv \ \lambda_m^{k_L(r)} \bmod L \quad \text{for } k_L(r) \equiv l_p(r), \text{ for all } p|\varphi(L), \tag{30}$$

$$(r/\lambda_r) \ \equiv \ (m/\lambda_m)^{k_L(r)} \bmod L. \tag{31}$$

We shall combine this strengthening with properties of dual elliptic pseudoprimes, which we introduce in the next section, with the goal of eliminating the final trial division (1) in cyclotomy tests of a given pair of dual elliptic primes.

5. Dual Elliptic Primes and Pseudo-primes

We start with the definition of the dual elliptic primes, which is, as mentioned in the introduction, related to the notion of twin primes in the rational integers.

Definition 10. *We say that two primes p and q are dual elliptic primes associated to an order $\mathcal{O} \subset \mathbb{K} = \mathbb{Q}(\sqrt{-d})$, if there is a prime $\pi \in \mathcal{O}$ such that $p = \pi \cdot \overline{\pi}$ and $q = (\pi + \varepsilon)\overline{(\pi + \varepsilon)}$ with $\varepsilon = \pm 1$.*

Dual elliptic primes *exist*: In the ECPP program, a special flag was introduced in order to skip dual pseudoprimes, which do not reduce the size of the numbers to be proved prime; it happens regularly that the flag is set [31]. Furthermore, empirical considerations of Galbraith and McKee [17] suggest they are sufficiently frequent, in order to develop efficient algorithms in which they are used. The problem of showing that dual elliptic primes have a satisfactorily asymptotic distribution is certainly much harder.

We define in the spirit of pseudoprimality followed from the introduction, a pair of dual elliptic pseudoprimes as follows:

Definition 11. *Let m and n be two strong pseudoprimes, $\mathcal{O} \subset \mathbb{K} = \mathbb{Q}(\sqrt{-d})$ an order in an imaginary quadratic extension and assume that there are two curves $\mathcal{E}_m(A, B)$, $\mathcal{E}_n(C, D)$ which are both associated to $\mathcal{O}$ in the sense of Definition 3. In particular, m, n are Atkin pseudoprimes. Furthermore, we assume that:*

1. *There are a point $P \in \mathcal{E}_m(A, B)[n]$ and a point $Q \in \mathcal{E}_n(C, D)[m]$ and the (Atkin) - sizes of the curves are*
$$|\mathcal{E}_m(A, B)| = n, \quad \text{and} \quad |\mathcal{E}_n(C, D)| = m.$$
2. *The sizes m and n factor in $\mathcal{O}$ as*
$$m = \mu\overline{\mu}, \quad \text{and} \quad n = (\mu + \varepsilon) \cdot \overline{(\mu + \varepsilon)}, \quad \text{with} \quad \varepsilon = \pm 1. \tag{32}$$
Note that from (14) we have that m, n are square-free.
3. *The polynomial $H_{\mathcal{O}}(X)$ has a root j_m modulo m, and a root j_n modulo n, and the curves $\mathcal{E}_m(A, B), \mathcal{E}_n(C, D)$ have invariants which are rational functions in these values.*
4. *Both m and n have no prime factor $p < 5$.*

If these conditions are fulfilled, the pair (m, n) is called a pair of dual elliptic pseudoprimes *associated to the order $\mathcal{O}$.*

Finding a point P on $\mathcal{E}_m(A, B)$ can be done by adapting a trick of [4, 8.6.3], thereby bypassing the problematic extraction of a square root modulo m. This works as follows: find $x_0 \bmod m$ for which $\lambda = x_0^3 + ax_0 + b \mod m$ is such that $\left(\frac{\lambda}{m}\right) = 1$. Then $P = (\lambda x_0, \lambda^2)$ is a point on the curve $Y^2 = X^3 + A\lambda^2 X + B\lambda^3$, which should be isomorphic to $\mathcal{E}_m(A, B)$ if m is actually a prime[4].

Practically, dual elliptic pseudoprimes are found by featuring a pair of strong pseudoprimes (m, n); the pseudoprime test may consist in taking the roots

[4] I thank F. Morain for this observation

$\sqrt{-d \bmod m}, \sqrt{-d \bmod n}$, operations which are anyhow necessary in the context. The integers m and n both split in a product of two principal primes in $\mathbb{K}$, such that there is a pair of factors which differ by ± 1. Once such pseudoprimes are found, the invariants j_m, j_n must be computed by methods explained in [34], [4]. Then the curves $\mathcal{E}_m(A,B), \mathcal{E}_n(C,D)$ can be built and points on these curves are chosen as explained above. The points are used in order to perform an elliptic pseudoprime test, as required in point 1 of the Definition 11. In practice one notes that, given a strong pseudoprime n, finding an appropriate order $\mathcal{O}$ and a dual elliptic pseudoprime m to n is a particular form of the first round of an elliptic curve primality test (ECPP) [34]. In particular, the heuristic arguments based upon [17] suggest that this step requires cubic time.

The easiest fact about dual elliptic pseudoprimes is the following:

Lemma 3. *Two dual elliptic pseudoprimes (m,n) associated to an order $\mathcal{O}$ are simultaneously prime or composite. Furthermore, if m,n are composite and $\mathcal{O} \subset \mathbb{K} = \mathbb{Q}(\sqrt{-d})$, then for any prime divisor $\ell | m \cdot n$ there is a $\lambda \in \mathcal{O}(\mathbb{K})$ such that $\ell = \lambda \cdot \overline{\lambda}$.*

Proof. Assume m is prime. Then item 1. of the Definition 11 requires also an elliptic Fermat primality proof for n. It implies that for any possible prime $q|n$, the curve $\mathcal{E}_q(\overline{A}, \overline{B}) = \mathcal{E}_n(A,B) \bmod q$ has a point of prime order $m > (\sqrt{n}-1)^2$. This cannot hold for primes $q < \sqrt{n}$ and thus n is prime too. Conversely, if n is prime, m is also prime by the same argument. This confirms the first statement.

Suppose now that m and n are composite and $\ell \in \mathbb{N}$ is a prime so that $\ell | n$, say. The condition (14) implies that n is square - free and Lemma 1 together with point 2. of the Definition 3 imply that ℓ splits in a product of principal ideals of $\mathcal{O}$, which completes the proof. □

We shall assume from now on, without restriction of generality, that $\varepsilon = 1$ in the Definition 11 (note that changing the sign of ε amounts to interchanging m and n). We prove that the tests required by the definition imply that, if dual elliptic pseudoprimes are composite, then their least prime factor *has* the dual elliptic prime property.

Theorem 3. *Let (m,n) be a pair of composite dual elliptic pseudoprimes associated to an order $\mathcal{O} \subset \mathbb{Q}(\sqrt{-d})$ and let $p \mid m$ be the least prime factor of m. Then there is a prime factor $q \mid n$, such that p, q are dual elliptic primes.*

Furthermore, if the prime q is not the least prime factor of n, then both m and n are built up of at least three prime factors.

Proof. By Definitions 4 and 11, there is a point $P \in \mathcal{E}_m(A,B)$ with $[n]P = \mathfrak{O}$. Let $\mathbf{P} = P \bmod p \in \mathcal{E}_p(\overline{A}, \overline{B}) = \mathcal{E}_m(A,B) \bmod p$; it has an order $h \mid n$. If h is a prime, then p, h are dual elliptic primes and the proof is completed. Let us thus assume that h is composite and $q \mid h \mid n$ is the least prime dividing h, so $h = q \cdot u$, with some $u > 1$. By the choice of q it follows that $q^2 < qu = h$. We then consider $Q \in \mathcal{E}_n(C,D)[m]$ and the point

$$\mathbf{Q} = (Q \bmod q) \in \mathcal{E}_q(\overline{C}, \overline{D}) = (\mathcal{E}_n(C,D) \bmod q)\,,$$

which must have a non trivial order $h' \mid m$, since Q is an $m-$th torsion point. The choice of p implies $h' \geq p$. Applying the Hasse inequalities to h and h' we find:

$$\begin{array}{rcccl} q^2 & \leq & q \cdot u & \leq & (\sqrt{p}+1)^2, \\ (\sqrt{p}-1)^2 & \leq & h & \leq & u^2, \\ p & \leq & h' & \leq & (\sqrt{q}+1)^2. \end{array}$$

Thus, from the first two lines, $q \leq \sqrt{p}+1 \leq u+2$ and combining to the other inequalities we have:

$$q \cdot u \leq (\sqrt{p}+1)^2 \leq (\sqrt{q}+1)^2 + 1 + 2\sqrt{p}.$$

After division by q, we find the following bonds on u:

$$1 \leq u \leq \frac{(\sqrt{q}+1)^2}{q} + \frac{2u+3}{q} < 1 + 4/q + 2/\sqrt{q} + 2u/q,$$

and since $q \geq 5$, also $3u/5 < 3$. This is impossible, since $u > q \geq 5$ is an integer. Thus $u = 1$ and $h = q$ is prime, which completes the proof of the second statement.

We had chosen q as the least prime factor of h, the order of the point $\mathbf{P} \in \mathcal{E}_p(A, B)$. We now show that if q is not the least prime factor of n, then n has more then two prime factors. Assume that $q' < q$ is the least prime dividing n. By the proof above, there is a prime $p' \mid m$ such (q', p') are dual; also the premises imply that $p' > p$. Given the double duality, we have the following factorizations in $\mathcal{O}(\mathbb{K})$:

$$\begin{array}{rclcrclcl} p & = & \pi \cdot \overline{\pi} & ; & q & = & \rho \cdot \overline{\rho} & = & (\pi+\delta)\left(\overline{\pi+\delta}\right) \\ p' & = & \pi' \cdot \overline{\pi}' & ; & q' & = & \rho' \cdot \overline{\rho}' & = & (\pi'+\delta')\left(\overline{\pi'+\delta'}\right), \end{array}$$

where $\delta,\ \delta' = \pm 1$ and π and π' can be chosen such that their traces be positive.

We assume that $m = p \cdot p'$ and $n = q \cdot q'$ and insert the last equations in the factorizations of m and n in $\mathbb{K}$:

$$\begin{array}{rcccrcl} m & = & \mu \cdot \overline{\mu} & \text{and} & \mu & = & \pi \cdot \pi' \\ n & = & (\mu+1) \cdot (\overline{\mu}+1) & \text{and} & \mu+1 & = & (\pi+\delta) \cdot (\pi'+\delta'). \end{array}$$

Subtracting the right hand side equations, we find $1 - \delta \cdot \delta' = \delta\pi' + \delta'\pi$. If $\delta = \delta'$, this implies $\pi + \pi' = 0$ and μ is a square. If $\delta = -\delta'$ then $\pi' - \pi = 2\delta$ and $\rho = \pi + \delta$, so $\rho' = \pi' + \delta' = \pi + 2\delta + \delta' = \pi + \delta = \rho$, then ν is a square. But both μ, ν were assumed square-free, a contradiction which confirms that at least one of m and n must have three factors.

Assume now that one of m, n is built up of two primes, say $m = p \cdot p'$, while $n = q \cdot q' \cdot q''$, where q'' is a factor which may be composite and $q' < q < q''; p < p'$. By duality, we have $q' > (\sqrt{p'}-1)^2$ and $q'' > q > (\sqrt{p}-1)^2$, thus

$$n = q \cdot q' \cdot q'' > m \cdot \left((p + 1 - 2\sqrt{p}) \cdot (1 - 2/\sqrt{p})(1 - 2/\sqrt{p'})\right).$$

For $p' > p \geq 11$ it follows that $n > 1.367\ m$ and $m > 121$, in contradiction with $n < m + 1 + 2/\sqrt{m} < 1.2\ m$. The remaining cases can be eliminated individually, using the fact that small primes $5 \leq p < 11$ split in principal ideals only in few imaginary quadratic extensions, and in those cases, if $p = \pi \cdot \overline{\pi}$, then $\pi \pm 1$ is not prime. □

An immediate consequence is the following:

Corollary 1. *Let (m,n) be dual elliptic pseudoprimes associated to the order $\mathcal{O} \subset \mathbb{K} = \mathbb{Q}(\sqrt{-d})$ and $k = k(m,n) = \max\{\Omega(m), \Omega(n)\}$, where $\Omega(x)$ denotes the number of prime factors of x, with repetition. Then there are two primes $p \mid m$ and $q \mid n$ such that:*

$$|p-q| < 2\sqrt{\max(p,q)} < 2\sqrt[2k]{\max(m,n)} \leq 2\sqrt[4]{\max(m,n)}. \tag{33}$$

Proof. Suppose that m has $k = k(m,n)$ factors and let p be its least prime factor, so $p < m^{1/k}$. Let q be the dual prime of p dividing n: the existence of q follows from the previous theorem. Then (33) follows from the duality of p and q and the bound on p. □

We finally show that dual elliptic primes with two factors might exist. This leads to a formula which reminds formulae for the prime factors of Carmichael numbers.

Theorem 4. *Let (m,n) be a pair of dual elliptic pseudoprimes associated to an order $\mathcal{O} \subset \mathbb{Q}[\sqrt{-d}]$ and suppose that both are built up of exactly two prime factors. Let $m = \mu \cdot \overline{\mu}$ and $n = (\mu+1)\cdot(\overline{\mu}+1)$ be the factorizations of m and n in $\mathbb{K}$. Then there is a prime π, an element $\alpha \in \mathcal{O}$ and a unit δ, such that:*

$$\begin{aligned} \nu &= (\pi+\delta)\cdot(\alpha\pi+\delta) \quad \textit{and} \\ \mu &= \pi\cdot(\alpha(\pi+\delta)+\delta). \end{aligned} \tag{34}$$

Proof. Let $m = p \cdot p'$ and $n = q \cdot q'$ be the rational prime factorization of m and n. Since m and n have only two prime factors, it follows from Theorem 3 that the least primes, say p, q must be dual to each other. So let $p = \pi \cdot \overline{\pi}$ and $q = \rho \cdot \overline{\rho} = (\pi+\delta)\cdot(\overline{\pi+\delta})$.

Let also $p' = \pi' \cdot \overline{\pi}'$ and $q' = \rho' \cdot \overline{\rho}'$. The size of $\mathcal{E}_{q'}(\overline{C}, \overline{D}) = \mathcal{E}_n(C,D) \bmod q'$ divides m and it follows, after an adequate rearrangement of conjugates, that there is an $\varepsilon = \pm 1$ such that $\rho' + \varepsilon$ is divisible by either π or π'.

If the divisor was π' we would reach a contradiction like in the last step of the proof of Theorem 3. Assume thus that $\rho' = \alpha\pi - \varepsilon$, the divisor being π. Symmetrically, $\pi' = \beta\rho + \varepsilon'$. First consider the splitting of ν:

$$\mu + 1 = \nu = \rho \cdot \rho' = (\pi+\delta)(\alpha\pi+\varepsilon) = \pi(\alpha\pi + \alpha\delta + \varepsilon) + \varepsilon\delta$$

Reducing the above equation modulo π, we conclude that $\varepsilon\delta = 1$ and thus $\varepsilon = \delta$, both factors being ± 1. Let us compare the two expressions for μ:

$$\mu = (\alpha\pi^2 + \delta(\alpha+1)\pi + 1) - 1 = \pi(\beta(\pi+\delta) + \varepsilon')$$

and, after dividing π out,

$$(\alpha - \beta)(\pi + \delta) = \varepsilon' - \delta.$$

If $\varepsilon' = \delta$, then $\alpha = \beta$ and the claim follows. If $\alpha \neq \beta$, one can divide both sides by $\alpha - \beta$:

$$\pi + \delta = \pm\frac{2}{\alpha - \beta}, \quad \text{thus} \quad (\alpha-\beta)|(2).$$

Assuming that $\alpha - \beta = \zeta \in \mathcal{O}(\mathbb{K})^\times$, one finds $\rho = \pi + \delta = 2\zeta'$, for some related root of unity ζ'. This contradicts the fact that $\rho\overline{\rho} = q \geq 5$.

Finally we have to consider the case when $\alpha - \beta \in \mathcal{O}$ divides 2 and is not a unit. The only quadratic imaginary extension in which the prime 2 factors in principal ideals is $\mathbb{K} = \mathbb{Q}[\imath]$. Thus for $\mathbb{K} \neq \mathbb{Q}[\imath]$ we must have $\alpha = \beta$ and the statement follows. Finally, if $\mathbb{K} = \mathbb{Q}[\imath]$, we substitute $\alpha - \beta = 1 \pm \imath$ in the previous identity

and find solutions for $\pi, \pi'; \rho, \rho'$ which are also of the shape (34); this completes the proof. □

5.1. **Elliptic extentions of dual elliptic pseudoprimes.** Let (m, n) be a pair of dual elliptic pseudoprimes associated to an order $\mathcal{O} \subset \mathbb{K} = \mathbb{Q}(\sqrt{-d})$ and $\mathcal{E}_m(A, B), \mathcal{E}_n(C, D)$ be the respective curves. We have shown that to the least prime $p|m$ there is a dual elliptic $q|n$ and both factor into principal primes in $\mathbb{Q}(\sqrt{-d})$; let $p = \pi \cdot \overline{\pi}$ and $(\pi + \delta)(\overline{\pi} + \delta) = q$ be these factorizations, with $\delta = \pm 1$. Suppose that L is a square free integer for which the L - torsions of the curves $\mathcal{E}_m(A, B)$ and $\mathcal{E}_n(C, D)$ give raise to elliptic extensions of $\mathbb{Z}/(m \cdot \mathbb{Z}), \mathbb{Z}/(n \cdot \mathbb{Z})$. Let these extensions be defined over the saturated $\varphi(L)-$th cyclotomic extensions $(\mathbf{R}_m, \zeta_m, \sigma_m)$ and $(\mathbf{R}_n, \zeta_n, \sigma_n)$ respectively.

If m, n are primes, then the eigenvalues of the Frobenius are $\mu + 1, \overline{\mu} + 1$ for Φ_m and $\mu, \overline{\mu}$ for Φ_n, as one deduces from the sizes of the curves. By definition of the Elkies primes, they split in $\mathcal{O}(\mathbb{K})$ and for each prime $\ell|L$ we have $(\ell) = \mathcal{L}_1 \cdot \mathcal{L}_2$; one should check additionally that:

$$\begin{aligned} \lambda_m &\in \{\mu + 1 \bmod \mathcal{L}_1, \overline{\mu} + 1 \bmod \mathcal{L}_1\}, \\ \lambda_n &\in \{\mu \bmod \mathcal{L}_1, \overline{\mu} \bmod \mathcal{L}_1\} .. \end{aligned} \tag{35}$$

Then (30) implies that there are two integers k, k' such that:

$$\pi \equiv \mu^k \bmod L\mathcal{O} \quad \pi + \delta \equiv (\mu + 1)^{k'} \bmod L\mathcal{O}.$$

Remark 4. *The numbers k, k' are determined by $k \equiv l_{v^i}(p)$ and $k' \equiv l_{v^i}(q)$ for each prime power $v^i || \varphi(L)$. Using also (23) both for m and n, it follows that*

$$(\mu + 1)^{k'} - \mu^k \equiv \delta \bmod L\mathcal{O}. \tag{36}$$

Note that the fact that the $\varphi(L)-$th extension is saturated requires in particular, that for each prime $v|\varphi(L)$ with saturation exponent j, the power $v^j|\varphi(L)$.

One may consider (36) as an equation in the unknowns k, k'. In particular, $(1, 1)$ is always a possible solution, for which $\delta = 1$. It is possible that for certain L, the trivial is the only solution. We shall say that a square free integer L, which is product of primes ℓ which split in $\mathcal{O}(\mathbb{K})$ and such that (36) has only the trivial solution is a **good** L – with respect to the dual pseudoprimes m, n. This property has important consequences for the cyclotomy test as shown by the following

Theorem 5. *Let m, n be dual elliptic pseudoprimes associated to an order $\mathcal{O} \subset \mathbb{K} = \mathbb{Q}[\sqrt{-d}]$ and let $m = \mu \cdot \overline{\mu},\ n = (\mu + 1)(\overline{\mu} + 1)$ be the respective factorizations in $\mathcal{O}$.*

Suppose that $L \in \mathbb{N}$ is a square free integer for which an $L-$th elliptic extension exists both for $\mathbb{Z}/(m \cdot \mathbb{Z})$ and $\mathbb{Z}/(n \cdot \mathbb{Z})$ and they are defined using the saturated $\varphi(L)$ extensions $(\mathbf{R}_m, \zeta_m, \sigma_m)$ and $(\mathbf{R}_n, \zeta_n, \sigma_n)$ respectively; suppose that (35) holds for the eigenvalues of these extensions. If the system (36) has only the trivial solution $(k, k') = (1, 1)$ and $p \mid m; q \mid n$ are two dual elliptic primes, then

$$l_v(p) \equiv l_v(q) \equiv 1 \bmod v^N, \quad \text{for each prime } v|\varphi(L) \text{ and } N > 0. \tag{37}$$

Proof. The statement (37) is a direct consequence of Remark 4 and the fact that the $\varphi(L)-$th extensions is saturated. □

The Theorem suggests the following procedure for eliminating the final trial division step in the cyclotomy test:

1. Start with a pair of dual elliptic pseudoprimes m, n associated to an order $\mathcal{O}$ and choose two parameters s, t with $s|(n^t - 1, m^t - 1)$ for a cyclotomy test, as indicated by Remark 3.
2. Search by trial and error a square free L such that $t|\varphi(L)$ and an elliptic $L-$th extension of $\mathbb{Z}/(m \cdot \mathbb{Z})$ and of $\mathbb{Z}/(n \cdot \mathbb{Z})$ exists. Note that the primes dividing L need to be Elkies primes, which depends on $\mathcal{O}$ and not on the individual values of m, n. They may but need not divide s.
3. Suppose that additionally (35) holds and (36) has only the trivial solution.

If such a construction succeeds together with the main stage of the cyclotomy test for m, n and these are not primes, then there are two (dual elliptic) primes $p \mid m; q \mid n$ with $p < \sqrt{m}, q < (\sqrt{p} + 1)^2$ and such that

$$p \equiv m \bmod L \cdot s \quad \text{and} \quad q \equiv n \bmod L \cdot s. \tag{38}$$

This follows from (37) together with the fact that the existence of an $Ls-$th cyclotomic is jointly proved by the cyclotomy test and the above additional steps. In particular, the final trial division is herewith superfluous.

5.2. **Heuristics.** We complete this section with a heuristic analysis for the odds of finding L which verifies the conditions of Theorem 5. We start with some simplifications and consider one prime $\ell|L$ with $\ell > 3$ and which factors in $\mathcal{O}$ according to $(\ell) = \mathcal{L}_1 \cdot \mathcal{L}_2$. We let $x \equiv \mu \bmod \mathcal{L}_1$ and $y \equiv \overline{\mu} \bmod \mathcal{L}_1$, with $x, y \in \mathbb{F}_\ell^\times$. Restricted to $L = \ell$, the system (36) becomes in this notation: $x^k + \delta = (x+1)^{k'}$ and $y^k + \delta = (y+1)^{k'}$. Fix a generator $g \in \mathbb{F}_\ell^\times$ and consider the discrete logarithm in $\mathbb{F}_\ell^\times$ with respect to g.

We shall assume for simplicity that $x, y, x{+}1, y{+}1$ also generate the multiplicative group $\mathbb{F}_\ell^\times$, so

$$\log(a) \in (\mathbb{Z}/\ell - 1 \cdot \mathbb{Z})^* \quad \text{for} \quad a \in \{x, y, x+1, y+1\}. \tag{39}$$

Consider the functions $f_x, f_y : \mathbb{Z}/(\ell - 1 \cdot \mathbb{Z}) \to \mathbb{Z}/(\ell - 1 \cdot \mathbb{Z})$ given by

$$f_x(k) = \frac{\log(x^k + \delta)}{\log(x+1)} \quad f_y(k) = \frac{\log(y^k + \delta)}{\log(y+1)}.$$

The system (36) is now $f_x(k) = f_y(k) = k'$. We exclude the couple $(1, 1)$, corresponding to the trivial solution, from the graph of f_x. Furthermore $x \neq 0 and x{+}1 \neq 0$, and thus $x^k \neq -\delta$ and $(x+1)^{k'} \neq \delta$. This excludes an additional pair (a, b) from the graph of f_x. The same holds for f_y and both maps are restricted to domains and codomains of equal size $\ell - 3$.

Fact 3. *Our heuristic is based on the assumption that the functions f_x, f_y are well modeled by random permutations of $S_{\ell-3}$. In particular, modulo a redefinition of either domain or codomain, the maps are invertible and the system (36) reduces to $f_y^{-1} \circ f_x(k) = k$. According to our model, the map $h_{x,y} = f_y^{-1} \circ f_x$ is also a random permutation and it should have at least one fixed point.*

The number of fixed points of random permutations is well understood: it has expected value 1 and is Poisson distributed. Asymptotically, the individual probabilities $P_k = P(h \text{ has } k \text{ fixpoints}) \to \frac{1}{k!}$. Along with the expected value, we are interested in the probability that h has no fix points at all, which is $P_0 = 1/e$. The $\limsup_{X \to \infty} \frac{X}{\varphi(X) \log\log(X)} \leq C$ for some $C > 0$, []. For fixed $x, y, x+1, y+1$ and a given $0 < B < \log(m)$, a prime $\ell \equiv 1 \bmod B$ such that (39) holds, occurs with

probability $P > C'/(\log\log(B))^4$. *The heuristic model implies that with expectation* $1/e$, *(36) will only have the trivial solution for such a prime.*

A further approach which can be analyzed with the same model is the following: choose ℓ_1, ℓ_2 *like above, and let* n_1, n_2 *be the respective number of fixed points. The expected values are* $n_1 = n_2 = 1$. *Suppose that* $(\ell_1 - 1, \ell_2 - 1) = d$ *and let* $k, k' \in \mathbb{Z}/(\varphi(L) \cdot \mathbb{Z})$ *be a non trivial solution of (36). Let* $k_i \equiv k \bmod \ell_i - 1$; $k_i' \equiv k' \bmod \ell_i - 1$, $i = 1, 2$ *be the exponents with respect to* ℓ_i. *They correspond to some of the* n_i *solutions modulo* ℓ_i, *and thus* $k_1 \equiv k_2 \bmod d$; $k_1' \equiv k_2' \bmod d$. *Since there is in average only one solution modulo each prime, this solution must verify the above pair of additional conditions, which are met with probability* $1/d^2$. *Thus, if* $d > 1$, *the probability that (36) has a solution for* L *as above is* $1/d^2 < 1/e$ *and trying at least two primes yields a stronger filtering.*

Certainly, the condition (39) is only necessary for a simpler heuristic argument. The analysis may become difficult when some of $x, y, x+1, y+1$ are not generators. The odds of finding a *good* L are though the same range of magnitude. For the purpose of finding good L, we thus propose the more general algorithm:

Algorithm ACE*(Auxiliary Cyclotomic & Elliptic Extensions)*

Input. m, n a couple of dual elliptic pseudoprimes with respect to $\mathcal{O}$ with given factorization; t, an exponent for a CPP test. *Output* L a square-free integer with $t|\varphi(L)$ and such that (36) has only the trivial solution modulo L. Compute a sequence of primes $\ell_i > 3$; $i = 1, 2, \ldots h$ and let $L_i = \prod_{j \le i} \ell_i$, such that

(i) $d_i = (\ell_i, \varphi(L_{i-1})) > 1$.
(ii) $L = L_h$ is such that $t|\varphi(L)$.
(iii) The equations (36) have no non trivial solutions modulo L.

Remark 5.

A. *We have implemented this algorithm. In most cases, the equations (36) had only the trivial solution for* L *a product of two primes. In more then one fourth of the cases, this happened already for one prime, and we encountered no case in which a product of more then three primes was necessary for a good* L. *Thus the experimental results in the general case are close to the heuristic predictions for the particular case in which (39) holds.*

B. *The condition (i) has the following purpose: in general, we reach a good* L_j *already for* $j \le 3$, *however the condition* $t|\varphi(L)$ *will not be fulfilled. Suppose thus that* L_j *is good and (36) has at least one non trivial solution* (k, k') *for* ℓ_{j+1}. *If* $d_{j+1} > 1$, *since* L_j *is good, we must have* $k \equiv k' \equiv 1 \bmod d_{j+1}$*: this allows filtering. In practice, one shall choose* d_j *to be at least divisible by some factors of* t.

C. *Assume that* $B > 0$ *is such that all prime power factors of* t *are* $< B$ *and the number of prime factors is also* $< B$ *– see (21). We claim that the Algorithm ACE will complete in average time* $O(B^{3+\varepsilon})$. *For the analysis, we use again the slower approach, in which one seeks for each prime power* $v|t$ *a good prime* $\ell \equiv \bmod v$, *such that (39) holds. By Fact 3, a good prime for which (39) holds occurs with probability* $O(1/\log\log^4(B))$. *Combining with the probability to find a prime* $\ell \equiv 1 \bmod v$ *estimated with the Linnick constant, we deduce that for sufficiently large* t *and thus* B, *there is a good*

prime $\ell(v) < B^{1+\varepsilon}$ with $\ell(v) \equiv 1 \bmod v$ for each prime power $v|t$. It tales $O(B^{2+\varepsilon})$ to find such a prime. Repeating this for all $v|t$ will take at most $O(B^{3+\varepsilon})$ operations, as claimed. In practice, by (21), $B = O(\log\log(m))$ and thus the time required by the ACE Algorithm is negligeable.

5.3. **On constructing Elkies factors.** We finally add some detail on the construction of the Elkies factors of $\ell-$th torsion polynomials ψ_ℓ. Let m, n be dual elliptic pseudoprimes as above and ℓ be an Elkies prime. We consider the ℓ - torsion polynomial of $\mathcal{E}_n(C, D)$, which should have $x = \mu \bmod \mathcal{L}_1$ as an eigenvalue, where $(\ell) = \mathcal{L}_1 \cdot \mathcal{L}_2$ is the splitting of ℓ in $\mathcal{O}(\mathbb{K})$. If n is prime, there is an Elkies factor verifying:

$$F(X^n) - F(g_x(X)) \equiv 0 \bmod F(X),$$

where g_x is the multiplication polynomial defined in (9) with respect to $\psi_\ell(X)$. For pseudoprime n, we let

$$\begin{aligned} h_1(X) &= X^n \quad \text{rem} \quad \psi_\ell(X), \\ h_2(X) &= \psi_\ell(g_x(X)) \quad \text{rem} \quad \psi_\ell(X) \quad \text{and} \\ F(X) &= \text{GCD } (\psi_\ell(X), h_1(X) - h_2(X)) . \end{aligned} \tag{40}$$

If $x^2 \equiv m \bmod \ell$, then the eigenvalue x is double and we may discard ℓ or use direct factorization, e.g. some variant of the Berlekamp algorithm [40], Chapter V., for finding an Elkies factor.

If $x^2 \not\equiv m \bmod \ell$ and $F(X)$ does not verify the defining conditions for an Elkies factor, then n must be composite, and the primality test would stop at this point. Otherwise $F(X)$ is a factor which can be used in proving existence of an $\ell-$th elliptic extension.

6. Applications to Cyclotomy

We now come to the application of dual elliptic pseudoprimes for the cyclotomy primality test. A first application of these pseudoprimes was given in [26] and it took advantage of the Corollary 1 and the implied fourth root order bound (33) on the difference between the smallest eventual divisors of (m, n); this was an improvement on methods for finding divisors in residue classes, like [22], [12].

By using elliptic extensions and Theorem 5, we are in the more pleasant situation, that trial division may be completely eliminated in the cyclotomy tests. The particularity of our new algorithm consists in the inhabitual fact that, for proving primality of one pseudoprime, it is more efficient to do so for *two pseudoprimes* simultaneously. Only this allows, of course, to use the strong implications of duality.

Suppose that n is a test number like before and a second strong pseudoprime $m < n$ was found, such that (m, n) are dual elliptic pseudoprimes with respect to the order $\mathcal{O} \subset \mathbb{K} = \mathbb{Q}(\sqrt{-d})$. We choose some parameters s, t with $s > 2n^{1/4}$ and $t = \lambda(s)$, the Carmichael function. Then we find a good L with the algorithm ACE and choose a divisor $s'|s$ such that for $S = s' \cdot L$, the inequality

$$|(\ m \text{ rem } S\ ) - (\ n \text{ rem } S\ )| > 2n^{1/4} \tag{41}$$

holds. Next one performs the main stage of the cyclotomy test for S, on *both* m and n and proves the existence of an $L-$th elliptic extension by verifying (24), (25) in the same working extensions used for the cyclotomy test. Since $t|\varphi(L)$ and equality is not necessary, some additional working extensions will in general be required. Note that in building elliptic Jacobi sums, one has also to check that the primes

involved are not exceptional conductors. If this happens, the respective $\ell|L$ should be replaced by a new one, keeping the properties of L valid.

The Theorem 3. implies that there is a prime $p < \sqrt{n},\ p|n$ and a dual elliptic q to p, which divides m. Furthermore, the algorithm ACE and (15) imply that

$$|p-q| = |(\ m \text{ rem } S\ ) - (\ n \text{ rem } S\ )| > 2n^{1/4},$$

in contradiction with (33) and it follows that m, n must be primes.

We formulate the strategy described above in algorithmic form.

Algorithm CIDE*(Cyclotomy Initialized by Dual Elliptic tests)*
Let n be a strong pseudoprime.

1. Find a dual elliptic pseudoprime m to n, with respect to an order $\mathcal{O} \subset \mathbb{K} = \mathbb{Q}[\sqrt{-d}]$, by using standard versions of ECPP. If none can be found (in affordable time), then stop or skip to a classical cyclotomy test for n.
2. Choose the parameters s, t, such that (41) is verified and $t = \lambda(s)$ ([27]).
3. Find a good L using algorithm ACE and let $S = L \cdot s'$, where s' is the smallest factor of s such that (41) is verified by S.
4. Construct saturated working extensions of $\mathbb{Z}/(m\cdot\mathbb{Z}), \mathbb{Z}/(n\cdot\mathbb{Z})$ for each prime $v|\varphi(L)$. Let $\mathbf{R}_m, \mathbf{R}_n$ be their compositum.
5. Perform in $\mathbf{R}_m$ respectively $\mathbf{R}_n$ the Jacobi sum tests (20) necessary for proving the existence of $S-$th cyclotomic extensions of $\mathbb{Z}/(n\cdot\mathbb{Z})$ and of $\mathbb{Z}/(m\cdot\mathbb{Z})$.
6. Compute the elliptic Jacobi sums related to formulae (24) and (25) for all $\ell|L$ and eventually replace ℓ if it is an exceptional conductor.
7. Perform in $\mathbf{R}_m$ respectively $\mathbf{R}_n$ the elliptic Jacobi sum tests implied by (24) and (25), which are necessary for proving the existence of $L-$th elliptic extensions of $\mathbb{Z}/(n\cdot\mathbb{Z})$ and of $\mathbb{Z}/(m\cdot\mathbb{Z})$.
8. Declare m and n prime if all the above tests are passed successfully.

6.1. **Run Time.** We split the computations for a CIDE - test for a probable prime $n \in \mathbb{N}$ in three main stages:

I. Find a dual elliptic pseudoprime m to n.
II. Perform cyclotomy tests for m, n.
III. Find an L with the ACE algorithm and prove the existence of an $L-$th elliptic extension for m and n.

If the Jacobi sums for the Step II. are computed in essentially linear time, e.g. by using the algorithm of Ajtai et. al. [3], then Step II. reduces to the main stage of the cyclotomy test. This stage is polynomial and takes $O(\log^3(n))$ binary steps [28]. As mentioned above, heuristic arguments suggest that Step I. also takes cubic time [36], [17].

We analyze the run time for the Step III using the heuristics in Fact 3. Let the bound B be defined by (21); the factors of L will be $\ell < B^2$ and their number is $< B$. For each factor, one has to perform some elliptic Jacobi sum tests, at most

$\log(B)$; the degree of the extensions where the tests are performed is also $< B^2$. Altogether, using $B = O(\log\log(n))$, this implies that Step III is performed in

$$O\left(\log^{2+\varepsilon}(n) \times B^{3+\varepsilon}\right) = O\left(\log^{2+\varepsilon}(n)\right)$$

binary operations. The Step III. is thus dominated by steps I and II. Hence, the run time of the algorithm CIDE is:

$$O\left(\log(n)^{3+\varepsilon}\right).$$

Remark 6. *Using the certification algorithm described in* [28]*, one can also provide primality certificates which can be verified in quadratic time. Note that this time is* ***unconditional*** *and can be achieved also if no certified Jacobi sum tables are available.*

7. Conclusions

Since the summer of 2002, the theoretical problem of primality proving is solved: *Primes is in P*, as Agrawal, Kayal and Saxena laconically put it the title of their magnificent paper [2]. Apart from the thus closed search for a polynomial time deterministic algorithm, there is an alternative question concerning primality proving. Namely: "How large general numbers can **currently** be proved on a computer"?

It is a general fact that provable algorithms are different from their practical versions, which, if they exist, may lose some or many of the theoretical advantages, but work conveniently in practice. Thus, the algorithm of Goldwasser and Kilian [18, 19] has been proved to terminate in random polynomial time for all but an exponentially thin set of inputs; it has hardly ever been implemented, for complexity reasons mentioned in the introduction. In exchange, the ideas of Atkin [4] led to the current wide spread version of ECPP [32], which works very well in practice. As already mentioned, the choice of the fields of complex multiplication is in this version such that no *proof* of polynomial time termination is known; however, the algorithm works very stably in practice and heuristic argument brought in [17] explain this fact.

The situation is even more bizarre with the cyclotomy test: from the complexity theoretical point of view, it should even not be taken into consideration, since it is over-polynomial. For the range of primes which are currently affordable for computer proofs, it works very efficiently. A fortiori, the combination of cyclotomy and elliptic curves provided by CIDE has good reasons to be the medium term provider of largest primality proofs and the generation of certificates which can be verified in quadratic time, as observed in Remark 6, is also an appealing novelty. Furthermore, the algorithm has random cubic run-time, based on the heuristics of [17] and the ones in Fact 3.

Finally, the test of Agrawal, Kayal and Saxena has, for computer implementation, a serious space problem. Even the nice idea of Berrizbeitia [7], [6, 5] which brings an important run - time improvement[5], does not remove this problem. It is not likely that primes larger then 500 decimal digits, say, will be proved in the near future with any variation of the AKS algorithm, *unless new ideas are found, for solving the space problem.*

In conclusion, it is a mathematically appealing and relevant goal, to seek for an efficient variant of AKS, while on the side of CPP, the construction of Jacobi sums

[5]see various forms of generalizations in [5], [6], [10], [35],

remains a small problem, which is interesting per se. The algorithm of Ajtai, Kumar and Sivakumar yields however a random polynomial solution which is satisfactorily in theory, while the LLL and PARI approaches may solve the practical problem for conceivable applications during the next years or even decades.

References

[1] L. Adleman and R. R. C. Pomerance. On distinguishing prime numbers from composite numbers. *Ann. Math.*, 117:173–206, 1983.

[2] M. Agrawal, N. Kayal, and N. Saxena. Primes is in p. *Annals of Math.*, pages 781–793, 2004.

[3] M. Ajtai, R. Kumar, and D. Sivakumar. A sieve algorithm for the shortest vector problem. In A. Pres, editor, *Proceedings of the 33-rd Symposium on Theory of Computing (STOC)*, pages 601–610, 2001.

[4] A. Atkin and F.Morain. Elliptic curves and primality proving. *Math. Comp.*, 61:29–68, 1993.

[5] R. Avanzi and P. Mihăilescu. Efficient "quasi"- deterministic primality test improving aks. submitted.

[6] D. J. Bernstein. Proving primality in essentially quartic random time. *Math. Comp.*, 76(257):389–403, January 2007.

[7] P. Berrizbeitia. Sharpening 'primes in p' for a large family of numbers. *Math. Comp.*, 74:2043–59, 2005.

[8] W. Bosma and M. der Hulst. *Primality proving with cyclotomy*. PhD thesis, Universiteit van Amsterdam, 1990.

[9] A. Bostan, F. Morain, B. Salvy, and R. Schost. Fast algorithms for computing isogenies between elliptic curves. *Math. Comp.*, 2007. to appear.

[10] Q. Cheng. Primality proving via one round in ECPP and one iteration in AKS. In D. Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, number 2729 in Lecture Notes in Comput. Sci., pages 338–348. Springer Verlag, 2003.

[11] H. Cohen and H.W.Lenstra Jr. Primality testing and jacobi sums. *Math. Comp.*, 48:297–330, 1984.

[12] D. Coppersmith, N. Howgrave-Graham, and S. V. Nagaraj. Divisors in residue classes, constructively.

[13] D. A. Cox. *Primes of the Form $x^2 + ny^2$*. Wiley & Sons, 1989.

[14] R. Crandall and C. Pomerance. *Prime Numbers - A Computational Perspective*. Springer, 2002.

[15] A. Enge and F. Morain. Comparing invariants for class fields of imaginary quadratic fields. In C. Fieker and D. R. Kohel, editors, *Algorithmic Number Theory*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 252–266. Springer-Verlag, 2002. Proceedings of the 5th International Symposium, ANTS-V, Sydney, Australia, July 2002.

[16] A. Enge and F. Morain. Fast decomposition of polynomials with known Galois group. In M. Fossorier, T. Høholdt, and A. Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 2643 of *Lecture Notes in Comput. Sci.*, pages 254–264, 2003. Proceedings, 15th International Symposium, AAECC-15, Toulouse, France, May 2003,.

[17] S. D. Galbraith and J. McKee. The probabilitythat the number of points on an elliptic curve over a finite field is prime. *Journal of London Mathematical Society*, 62:671–684, 2000.

[18] S. Goldwasser and J. Kilian. Almost all primes can be quickly certified. In *Proc. 18-th Annual ACM Symp. on Theory of Computing*, pages 316–329, 1986.

[19] S. Goldwasser and J. Kilian. Primality testing using elliptic curves. *Journal of the ACM*, 46(4):450–472, July 1999.

[20] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Springer Graduate Texts in Mathematics*. Springe, 1990. Second Edition.

[21] H. W. Lenstra Jr. Primality testing algorithms (after adleman, rumely and williams). In *Seminaire Bourbaki # 576*, volume 901 of *Lectures Notes in Mathematics*, pages 243–258, 1981.

[22] H. W. Lenstra Jr. Divisors in residue classes. *Math. Comp.*, pages 331–334, 1984.

[23] H. W. Lenstra Jr. *Galois Theory and Primality Testing*, chapter 12, pages 169–189. Number 1142 in Lecture Notes in Mathematics. Springer Verlag, 1985.

[24] H. W. Lenstra Jr, October 2002. Seminar lectures in Leiden and Oberwolfach.

[25] H. W. Lenstra, Jr. and C. Pomerance. Primality testing with gaussian periods.

[26] P. Mihăilescu. *Cyclotomy of Rings & Primality Testing*. PhD thesis, ETH Zürich, 1997.
[27] P. Mihăilescu. Cyclotomy primality proving - recent developments. In *Proceedings of the Third International Symposium ANTS III, Portland, Oregon*, volume 1423 of *Lecture Notes in Computer Science*, pages 95–111, 1998.
[28] P. Mihăilescu. Cyclotomy primality proofs and their certificates. *Mathematica Gottingensis*, 2006.
[29] P. Mihăilescu, F. Morain, and E. Schost. Computing the eigenvalue in the schoof - elkies - atkin algorithm using abelian lifts. In *ISSAC*, 2007.
[30] P. Mihăilescu and V. Vuletescu. Elliptic gauss sums and counting points on curves, 2007.
[31] F. Morain. private communication.
[32] F. Morain. Site for downloading the elliptic curve primality test software of f .morain.".
[33] F. Morain. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. *Journal de Théorie des Nombres, Bordeaux*, 7:255–282, 1995.
[34] F. Morain. Primality proving using elliptic curves: An update. In *Proceedings of the Third International Symposium ANTS III, Portland, Oregon*, volume 1423 of *Lecture Notes in Computer Science*, pages 111–127, 1998.
[35] F. Morain. La primalité en temps polynomial [d'après adleman, huang; agrawal, kayal, saxena]. In *Seminaire Bourbaki 55-ème année*, number 917 in Lectures Notes in Mathematics, 2002-2003.
[36] F. Morain. Implementing the asymptotically fast version of elliptic curve primality proving algorithm. *Math. Comp*, 76(257), January 2007.
[37] R. Pinch. Galois module structure of elliptic functions. In O. U. Press, editor, *Computers in mathematical research (Cardiff, 1986)*, number 14 in Inst. Math. Appl. Conf., pages 69–91, 1988. New Series.
[38] R. Schoof. Counting points on elliptic points over finite fields. *J. Th. Nombr. Bordeaux*, 7:363–397, 1995.
[39] J. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 1996.
[40] J. von zur Gathen and J. Gerhardt. *Modern Computer Algebra*. Cambridge University Press, 2-nd ed. edition, 2000.
[41] L. Washington. *Elliptic Curves - Number Theory and Cryptography*. Chapman and Hall/CRC, 2003.

Mathematisches Institut der Universität Göttingen
E-mail address: preda@uni-amth.gwdg.de